

## **LISTING OF PENDING CLAIMS**

The following is a listing of the currently pending claims in this application:

1           1. (Currently Amended) A communications network security method for  
2   ascertaining the integrity of a first communications network and identifying potential  
3   security risks across a perimeter of the first communications network, the method  
4   comprising:

5           identifying a plurality of routes that define ~~a~~the first communications network;  
6           identifying a plurality of hosts associated with the first communications network  
7   as a function of the plurality of routes;

8           receiving a census of the first communications network as a function of the  
9   plurality of hosts to determine a topology of the first communications network;

10          probing at least one first host of the plurality hosts of the first communications  
11   network by transmitting a packet to the first host, the first host being selected from the  
12   census results and the packet having at least a source address of a second host which is  
13   associated with a second communications network, wherein the source address is selected  
14   independent of any request from the second host to the first host; and

15          determining a security characteristic of the probed first host as a function of a  
16   response by the probed first host in receiving the packet, the security characteristic being  
17   a measure of connectivity between the first communications network and the second  
18   communications network, the measure of connectivity being an indication of connectivity  
19   between the first communications network and the second communications network.

1           2. (Currently Amended) The method of claim 1 wherein the source address of the  
2   second host is an a return IP address associated with a host external to the first  
3   communications network, ~~and the external host being associated with the second~~  
4   communications network.

1           3. (Currently Amended) The method of claim 2 wherein the response of the  
2   probed first host to the receipt of the packet includes transmitting a second packet, the

3 second packet being derived using at least a portion of information from the received  
4 packet.

1 4. (Cancelled).

1 5. (Cancelled).

1 6. (Currently Amended) The method of claim 5-2 wherein the measure of  
2 connectivity is determined by the further operation of:

3 monitoring the probed first host to determine the response, and if the response  
4 includes a transmission of a second packet from the probed first host to the second host at  
5 the return IP address, generating a security alert message identifying the probed first host  
6 as a security risk.

1 7. (Previously Presented) The method of claim 3 wherein the first  
2 communications network and the second communications network have different security  
3 levels.

1 8. (Previously Presented) The method of claim 3 wherein the transmitted packet  
2 is a TCP packet which returns a TCP packet in response thereto.

1 9. (Previously Presented) The method of claim 3 wherein the second packet is a  
2 UDP packet or an ICMP packet, which returns either a UDP packet or ICMP packet in  
3 response thereto.

1 10. (Currently Amended) A method for analyzing network security across a  
2 perimeter of a first communications network utilizing a security host, the method  
3 comprising:

4 receiving a census of the first communications network;

5 transmitting, from the security host, a packet ~~from~~ associated with a host of a  
6 second communications network to a particular one host of a plurality of hosts internal to

7 the first communications network, the internal host being selected from the census, and  
8 the packet ~~being generated as a function of both~~ having an IP source address associated  
9 with the host of the second communications network, wherein ~~and an IP address~~  
10 ~~associated with the internal host of the first communications network~~ the IP source  
11 address is selected independent of any request from the host of the second  
12 communications network to the internal host of the first communications network; and

13 determining a security characteristic of the particular one internal host of the first  
14 communications network as a function of a response by the internal host to the receipt of  
15 the packet, the security characteristic being a measure of connectivity between the first  
16 communications network and the second communications network, the measure of  
17 connectivity being an indication of connectivity between the first communications  
18 network and the second communications network.

1 11. (Currently Amended) The method of claim 10 wherein the measure of  
2 connectivity is a function of whether the internal host of the first communications  
3 network communicates with the host of the second communications network, and the  
4 measure of connectivity being determined by the further operation of:

5 monitoring the internal host to determine the response, and if the response  
6 includes a transmission of a second packet, utilizing the IP source address, from the  
7 internal host to the host of the second communications network, generating a security  
8 alert message identifying the internal host as a security risk.

1 12. (Original) The method of claim 11 wherein the second packet is derived  
2 using at least a portion of information from the transmitted packet.

1 13. (Cancelled).

1 14. (Previously Amended) The method of claim 12 wherein the internal host is a  
2 dual-homed host.

1           **15.** (Previously Presented) The method of claim 11 wherein the security  
2 characteristic includes an indication that the internal host is outside any security measures  
3 provided by a firewall associated with the first communications network.

1           **16.** (Currently Amended) A communications system for ascertaining the integrity  
2 of a first communications network and identifying potential security risks across a  
3 perimeter of the first communications network, the communications system comprising:

4               a first plurality of computers associated with a the first communications network;  
5               a second plurality of computers associated with a second communications  
6 network; and

7               a security host computer which determines a security characteristic of a first  
8 computer from the first plurality of computers, the security characteristic being a measure  
9 of connectivity between the first communications network and the second  
10 communications network by probing the first computer by transmitting a packet to the  
11 first computer, the first computer being selected from a census of the first  
12 communications network and the packet being generated as a function of both an IP  
13 source address associated with a second computer of the second plurality of computers,  
14 wherein said IP source address is selected independent of any request from the second  
15 computer to the first computer, and an IP address associated with the first computer, and  
16 determining the measure of connectivity as a function of a response of the first computer  
17 to receiving the packet, the measure of connectivity being an indication of connectivity  
18 between the first communications network and the second communications network.

1           **17.** (Original) The communications system of claim 16 wherein the security host  
2 computer is associated with the first communications network.

1           **18.** (Previously Presented) The communications system of claim 17 wherein the  
2 response of the first computer to the receipt of the packet includes transmitting a second  
3 packet, the second packet being derived using at least a portion of information from the  
4 received packet.

1           **19.** (Previously Presented) The communications system of claim 18 wherein the  
2 security host computer determines the measure of connectivity by monitoring the probed  
3 first computer to determine the response, and if the response includes the transmission of  
4 the second packet from the probed host, generating a security alert message identifying  
5 the first computer as a security risk.

1           **20.** (Previously Presented) The communications system of claim 17 wherein the  
2 first communications network is an intranet and the second communications network is  
3 an Internet, and the first communications network and the second communications  
4 network have different security levels.

1           **21.** (Currently Amended) A security host computer for ascertaining the integrity  
2 of a first communications network and identifying potential security risks across a  
3 perimeter of the first communications network, the security host computer comprising:

4           means for performing a census of ~~a~~the first communications network and  
5 determining a topology of the first communications network, the topology being defined  
6 by at least one computer,

7           means for probing the at least one computer by transmitting a packet to the  
8 computer, the computer being selected from the census results and the packet being  
9 generated as a function of (i) the topology, (ii) an IP source address associated with a  
10 particular host computer associated with a second communications network, wherein the  
11 IP source address is selected independent of any request from the second computer to the  
12 first computer, and (iii) an IP address associated with the computer, the second  
13 communications network being separate from the first communications network; and

14           a monitor for determining a security level of the computer as a function of a  
15 response by the computer to the receipt of the packet, and the security level being a  
16 measure of connectivity between the first communications network and the second  
17 communications network, the measure of connectivity being an indication of connectivity  
18 between the first communications network and the second communications network.

1           **22.** (Currently Amended) The security host computer of claim 21 wherein the  
2 measure of connectivity is determined by monitoring the computer's response, and if the  
3 response includes a transmission of a second packet, utilizing the IP source address, from  
4 the computer, a security alert message identifying the computer as a security risk is  
5 generated.

1           **23.** (Previously Presented) The security host computer of claim 22 wherein the  
2 first communications network and the second communications network have different  
3 security levels.

1           **24.** (Currently Amended) A machine-readable medium having stored thereon a  
2 plurality of instructions, the plurality of instructions including instructions that, when  
3 executed by a machine, cause the machine to perform of a method for analyzing a first  
4 communications network's integrity and identifying potential security risks across a  
5 perimeter of the first communications network by receiving a census of the first  
6 communications network; probing a first host of the first communications network by  
7 transmitting a packet to the first host, the host being selected from the census results and  
8 the packet being derived as a function of a topology of the first communications network  
9 and the packet having a source address which is associated with a second host of a second  
10 communications network, wherein the source address is selected independent of any  
11 request from the second host to the first host; and determining the first communications  
12 network's integrity as a function of a response by the probed host in receiving the packet  
13 wherein the response indicates a measure of connectivity between the first  
14 communications network communicates and the second communications network, and  
15 the measure of connectivity being an indication of connectivity between the first  
16 communications network and the second communications network.

1           **25.** (Cancelled ) .

1           **26.** (Currently Amended) The machine-readable medium of claim 24 wherein the  
2 response of the probed first host to the receipt of the packet includes transmitting a

3 second packet, the second packet being derived using at least a portion of information  
4 from the received packet.

1           **27.** (Previously Presented) The machine-readable medium of claim 26 wherein  
2 the first communications network is an intranet, and the second communications network  
3 is an Internet.